CLAIMS

What is claimed is:

1. A method comprising:

programming a chip secret key into a manufactured chip;

sending the manufactured chip to a system original equipment manufacturer (OEM); and

generating at least one private key for the manufactured chip according to a received key update request.

2. The method of claim 1, wherein prior to programming the chip, the method comprises:

gathering unique identification (ID) information of the manufactured chip;

encrypting the identification information using a first key to form a chip ID for the manufactured chip; and

encrypting the chip ID using a second key to form the chip secret key.

3. The method of claim 2, wherein the unique identification information includes a wafer serial number of a wafer from which the chip is formed and an X,Y coordinate location of the manufactured chip within the wafer.

4. The method of claim 1, wherein a key size of the chip secret key is less than a key size of an asymmetric crypto-system private key.

5. The method of claim 1, wherein programming the chip secret key comprises:

storing the chip secret key within chip fuses of the manufactured chip; and

blowing selected fuses of the manufactured chip to prevent unauthorized access to the chip secret key.

6. The method of claim 1, wherein generating the private further comprises:

receiving the key update request from the system OEM;

authenticating the received key update request;

generating cipher text including the at least one private key for the manufactured chip if the key update request is authentic; and

sending the cipher text to the system OEM.

7. The method of claim 6, wherein authenticating the received key update request comprises:

verifying a digital signature of the system OEM included within the key update request;

decrypting the key update request to form a decrypted chip ID if the digital signature of the OEM is verified;

verifying that the chip ID of the manufactured chip matches the decrypted chip ID; and

disregarding the received key update request if the decrypted chip ID is not verified.

8. The method of claim 6, wherein generating the cipher text comprises:

generating a key vector including the at least one private key.

9. The method of claim 8, wherein generating the key vector comprises:

encrypting a unique secret value using the chip secret key to form the key vector;

removing all revoked keys from the key vector to form a private key vector; and

encrypting the private key vector, the chip ID and a digital certificate of the private key vector using the chip secret key and an initialization vector to form the cipher text.

10. The method of claim 1, wherein generating the at least one private key comprises:

generating cipher text including the at least one private key using an initialization vector (IV); and

sending the cipher text to the system OEM including the IV used to form the cipher text.

11. An article of manufacture including a machine readable medium having stored thereon instructions which may be used to program a system to perform a method, comprising:

programming a chip secret key into a manufactured chip;

sending the manufactured chip to a system original equipment manufacturer (OEM); and

generating at least one private key for the manufactured chip according to a received key update request.

12. The article of manufacture of claim 11, wherein prior to programming the chip, the method comprises:

gathering unique identification (ID) information of the manufactured chip;

encrypting the identification information using a first key to form a chip ID for the manufactured chip; and

encrypting the chip ID using a second key to form the chip secret key.

13. The article of manufacture of claim 11, wherein generating the private further comprises:

receiving the key update request from the system OEM;

authenticating the received key update request;

generating cipher text including the at least one private key for the manufactured chip if the key update request is authentic; and

sending the cipher text to the system OEM.

14. The article of manufacture of claim 11, wherein authenticating the received key update request comprises:

verifying a digital signature of the system OEM included within the key update request;

decrypting the key update request to form a decrypted chip ID if the digital signature of the OEM is verified;

verifying that the chip ID of the manufactured chip matches the decrypted chip ID; and

disregarding the received key update request if the decrypted chip ID is not verified.

15. The article of manufacture of claim 11, wherein generating the at least one private key comprises:

encrypting a unique secret value using the chip secret key to form the key vector;

removing all revoked keys from the key vector to form a private key vector; and

encrypting the private key vector, the chip ID and a digital certificate of the private key vector using the chip secret key and an initialization vector to form the cipher text.

16. An article of manufacture including a machine readable medium having stored thereon instructions which may be used to program a system to perform a method, comprising:

initializing an integrated chip to generate a key update request using a preprogrammed chip secret key stored within the integrated chip;

transmitting the key update request to a key distribution facility (KDF); and

storing received cipher text including at least one private key from the KDF

17. The article of manufacture of claim 16, wherein initializing the integrated chip comprises:

providing random cipher text to the integrated chip;

requesting the integrated chip to generate the key update request; and

attaching a digital signature of the random cipher text to the key update request.

18. The article of manufacture of claim 17, wherein requesting the integrated chip further comprises:

decrypting, by the integrated chip, the random cipher text using the chip secret key to form a random ID, a random key and a random digital certificate; and

encrypting, by the integrated chip, the random ID, the chip secret key and a pad value using a public key of the KDF to form the key update request.

19. The article of manufacture of claim 16, further comprising:

providing, during initial boot, the received cipher text to the integrated chip; and

decrypting, by the integrated chip, the received cipher text using the chip secret key to form a chip ID and the at least one private key; and

authenticating, by the integrated chip, with a content protection application to receive protected content.

20. The article of manufacture of claim 16, wherein the method further comprises:

providing the received cipher text to the integrated chip, the cipher text including the at least one private key, a key certificate and a chip ID assigned to the integrated chip in encrypted format using the chip secret key;

requesting the integrated chip to generate a key update request;

encrypting, by the integrated chip, the chip ID, the chip secret key and a random pad value using a public key of the KDF to form a second key update request; and

transmitting the second key update request to the KDF.

21. A method comprising:

initializing an integrated chip within a system to generate a key update request using a preprogrammed chip secret key stored within the integrated chip;

transmitting the key update request to a key distribution facility (KDF); and

storing received cipher text including at least one private key from the KDF.

22. The method of claim 21, wherein initializing the integrated chip comprises:

providing random cipher text to the integrated chip;

requesting the integrated chip to generate the key update request; and

attaching a digital signature of the random cipher text to the key update request.

23. The method of claim 22, wherein requesting the integrated chip further comprises:

decrypting, by the integrated chip, the random cipher text using the chip secret key to form a random ID, a random key and a random digital certificate; and

encrypting, by the integrated chip, the random ID, the chip secret key and a pad value using a public key of the KDF to form the key update request.

24. The method of claim 21, wherein storing the received cipher text comprises:

receiving an initialization vector (IV) with the received cipher text from the KDF; and

saving the received cipher text and the IV within off-chip persistent storage.

25. The method of claim 21, further comprising:

providing, during initial boot, the received cipher text to the integrated chip; and

decrypting, by the integrated chip, the received cipher text using the chip secret key to form a chip ID and the at least one private key; and

authenticating, by the integrated chip, with a content protection application to receive protected content.

26. The method of claim 25, wherein authenticating further comprises:

using, by the integrated chip, a private key digital certificate to authenticate with the content protection application.

27. The method of claim 25, wherein providing further comprises:

disabling access to the received cipher text following the initial boot.

28. The method of claim 21, wherein the KDF is a manufacturer of the chip.

29. The method of claim 21, further comprising:

providing the received cipher text to the integrated chip, the received cipher text including the at least one private key, a private key digital certificate and a chip ID assigned to the integrated chip in encrypted format using the chip secret key;

requesting the chip to generate a key update request;

encrypting, by the integrated chip, the chip ID, the chip secret key and a pad value using a public key of the KDF to form a second key update request; and

transmitting the second key update request to the KDF.

30. The method of claim 29, wherein the received cipher text includes a key vector including a series of non-unique private keys.

31. An integrated chip, comprising:

key request logic to generate a key update request using a preprogrammed chip secret key stored within the integrated chip to receive at least one private key from a key distribution facility (KDF).

32. The chip of claim 31, further comprising:

a first cryptographic block to decrypt received random cipher text using the chip secret key to form a random ID, a random private key and a random digital certificate; and

a second cryptographic block to encrypt the random ID, the chip secret key and a pad value using a public key of the KDF to form the key update request.

33. The integrated chip of claim 31, further comprising:

a first cryptographic block to decrypt received initialization cipher text using the chip secret key to form a chip ID, the at least one private key and a digital certificate.

34. The integrated chip of claim 31, comprising:

authentication logic to perform authentication with a content protection application to receive protected content using the digital certificate to avoid disclosing the identity of the integrated chip during the authentication.

35. The integrated chip of claim 33, wherein:

the initialization cipher text includes a key vector including a series of non-unique private keys.

36. A system comprising:

a flash memory;

an integrated chip including key logic to generate a key update request using a preprogrammed secret key stored within the integrated chip to receive at least one private key from a key distribution facility (KDF);

a processor coupled to the integrated chip; and

a storage device coupled to the processor, having sequences of instructions stored therein, which when executed by the processor, the processor is caused to initialize the integrated chip to generate the key update request, to transmit the key update request to the KDF and to store received cipher text including the at least one private key received from the KDF within the flash memory.

37. The system of claim 36, wherein the processor is further caused to provide during initial system boot the received cipher text to the integrated chip and to disable access to the received cipher text following the initial system boot.

38. The system of claim 36, wherein the processor is further caused to receive an initialization vector (IV) used to form the received cipher text with the received cipher text from the KDF and to save the received cipher text and the IV within a flash memory.

39. The system of claim 36, wherein the KDF is a manufacturer of the integrated chip.

40. The system of claim 36, wherein the received cipher text includes a key vector including a series of non-unique private keys.